Vol. 4, No. 1, 2018

УДК 327.88

ІНФОРМАЦІЙНА ВІЙНА РОСІЇ ПРОТИ УКРАЇНИ: ОСОБЛИВОСТІ ТА МЕХАНІЗМИ ПРОТИДІЇ

Микола Бучин
Національний університет "Львівська політехніка"
buchyn@ukr.net
ORCID: 0000-0001-9087-5123

Юля Курус
Національний університет "Львівська політехніка"
yuliia.kurus@gmail.com
ORCID: 0000-0002-3596-7073

(стаття надійшла до редколегії – 18.12.2017 р., прийнята до друку – 19.04. 2018 р.)

Розглянуто проблему інформаційної війни Росії проти Україні. Автори розкривають суть інформаційної війни, її трактування в межах широкого та вузького підходів. На основі використання історичного, системного та структурно-функціональних методів з'ясовано основні недоліки інформаційної сфери України, виокремлено основні механізми її захисту. Серед механізмів протидії інформаційній війні Росії проти України виділено дві групи: нормативно-правові та інституційні. До першої групи автори з0араховують законодавчі акти України, серед яких провідну роль у протидії інформаційній агресії Росії відіграє Доктрина інформаційної безпеки України. Серед другої групи механізмів дослідники виділяють державні та недержавні інституції, діяльність яких спрямована на формування та реалізацію інформаційної безпеки України, а також міжнародні структури, діяльність яких спрямована на нейтралізації інформаційного впливу з боку Росії. Серед вітчизняних інституційних механізмів протидії російській інформаційній важливе місце, на думку авторів, належить Міністерству інформаційної політики України, Раді національної безпеки та оборони України, кіберполіції та ін.

Значну увагу звертають на такі механізми протидії інформаційній війні Росії проти України, як заборона російських сайтів та соціальних мереж, а також запровадження квот на українську мову у мас-медіа. Автори зазначають, що дії України щодо нейтралізації інформаційних загроз з боку Росії слід здійснювати на трьох рівнях: перший – геополітичний (полягає у впливі на інформаційного агресора та обмеження інтенсивності і сили його нападу); другий – стан, який охоплює захист цілісності, ефективності та дієздатності системи управління, інформаційної інфраструктури, інформаційних ресурсів; третій – рівень громадськості (спрямований на захист стабільності та послідовності розвитку соціальних та політичних відносин, свідомості громадян, цілісності кожної людини).

Ключові слова: *інформаційна війна, інформаційна безпека, інформаційна стратегія, Росія, Україна*.

RUSSIAN INFORMATION WAR AGAINST UKRAINE: PECULIARITIES AND MECHANISMS OF COUNTERING

Mykola Buchyn
Lviv Polytechnic National University
buchyn@ukr.net
ORCID: 0000-0001-9087-5123

Yuliia Kurus
Lviv Polytechnic National University
yuliia.kurus@gmail.com
ORCID: 0000-0002-3596-7073

The article deals with the problem of Russian information war against Ukraine. The authors explain the primary sense of the information war, its interpretation in the framework of wide and narrow approaches. Basing on the use of

historic, systemic and structural-functional methods, the main disadvantages of the information sphere of Ukraine and the central mechanisms of its protection are identified. The tools of counteraction to the Russian information war against Ukraine are divided into two groups: legislative and institutional. To the first group there are referred the legislative acts of Ukraine, among which the Doctrine of Information Security of Ukraine that plays a leading role in counteracting Russian information aggression. Among the second group of mechanisms there are state and non-state institutions, whose activities are aimed at the formation and implementation of Ukraine's information security, as well as international structures whose actions are aimed at neutralizing the information influence from Russia. According to the authors, among the domestic institutional mechanisms of counteracting the Russian information war, the important place is taken by the Ministry of Information Policy of Ukraine, the National Security, and Defense Council of Ukraine, the Cyber Police, and others.

Considerable attention in the article is paid to such mechanisms of counteraction to Russian information war against Ukraine as the prohibition of Russian sites and social networks, as well as the introduction of quotas on the Ukrainian language in the mass media. The authors note that Ukraine's actions on the neutralization of information threats from Russia should be carried out at three levels: the first one – geopolitical (that is influencing the aggressor's information and limiting the intensity and force of his attack); the second – a state one that includes the protection of the integrity, efficiency and capacity of the management system, information infrastructure, information resources; the third – the level of the public (aimed at protecting the stability and consistency of the development of social and political relations, the consciousness of citizens, the integrity of each person).

Keywords: *information warfare, information security, information strategy, Russia, Ukraine.*

After the Revolution of Dignity that declared the desire of Ukrainians to live in a democratic European state, Ukraine became a victim of Russian armed aggression, resulting in the annexation of Crimea and military actions in Donbas, which continue to this day. Scientists describe activities of the Russian Federation against Ukraine as the hybrid war, which involves a combination of traditional and non-traditional methods of aggression, the complexity of aggressive actions in many areas of public life.

Information is one of the components of Russian aggression against Ukraine that allows speaking about the existence of an information war between Ukraine and Russia. It concerns active dissemination of negative (often false or distorted) information about Ukraine from the Russian Federation side to discredit our state, cyber-attack, propaganda of Russian values among the population of Ukraine, etc. This situation threatens the sovereignty and national security of Ukraine, as well as necessities of the development of mechanisms for counteracting the threats to the national security of our country in general, and information security, in particular.

The relevance of the chosen problem for research is also due to the insufficient level of scientific analysis of information warfare as a phenomenon inherent in contemporary international relations. There is still no single consistent interpretation of the notion of "information war", its features, structure, and mechanisms of counteraction in political science. Moreover, the research of information warfare is usually carried out at the level of journalism or political analytics, which requires more thorough scientific study of the essence of the phenomenon and the development of mechanisms for counteracting Russian information war against Ukraine at the present stage.

Such domestic researchers, as S. Demydyuk, N. Elyashevska, I. Lubkovych, M. Senchenko, are interested in the issues of Russian information war against Ukraine. P. Dibb, M. Kofman, Ch. Lamba and S. Rastorguiev are the foreign scholars who are studying the information warfare problem as well. The mentioned researchers analyze the essence and features of the information war as a phenomenon, consider the information war of Russia against Ukraine, study the threats that it carries both for Ukraine and the world community. At the same time, insufficient attention is paid to the research and development of mechanisms for counteracting the Russian information war at the present stage. The absence of a comprehensive study of Russian information war against Ukraine, and also the fact that Russia's aggression against our country in the information sphere continues and acquires new forms, requires more thorough research in this area.

The research aims are to carry out a political analysis of Russian information war against Ukraine and the mechanisms of its counteraction at the present stage.

For the present day, scientists have not formed a prevailing opinion regarding the scientific and theoretical concept of information wars, as well as the primary methods, forms and methods of their conduct. It should also be noted that information warfare is an ambiguous concept. Therefore, we can talk about the broad and narrow meaning of this term. In a general sense, information warfare is understood as any negative informational impact on the enemy. An opponent can be any subject: an individual or a group of persons, legal entities or the state. Participants in such wars can act individually or in groups, spontaneously or by agreement.

In the narrow sense, information warfare is a new type or method of armed conflict that is not subject to

international legal qualifications. However, there is no single opinion among scholars as most of them believe that the information war can't be considered as an armed conflict. This is because although information acts as a weapon, it can defeat the enemy without losing human lives and bloodshed [Lamb 1997].

In general, the broadest and most comprehensive definition of information warfare is, in our opinion, the following: information warfare is an open or latent targeted information impact of systems for each other to obtain a particular win in the political, economic or ideological sphere [Расторгуев 1997: 64–66].

Today, for Ukraine, during the informational confrontation with the Russian Federation, the protection of its own information space and national information security is one of the most important goals of the state governance, as well as the first step towards the formation of a positive image of the state on the world stage, successful European integration and the development of a self-sustaining, national self-identity.

The great Russian information war against Ukraine had entered a new stage at the beginning of 2014, when such events as the Revolution of Dignity, the annexation of the Crimea and the war in the East of Ukraine took place. To be honest, this confrontation illustrated: firstly, all vulnerable areas of Ukraine in information security; secondly, the lack of effectiveness of information security mechanisms; thirdly, unwillingness to unexpected and unpredictable information countermeasures.

Undoubtedly, the Ukrainian information sector has many disadvantages in the countering the information warfare. To determine the effectiveness of mechanisms that Ukraine uses to counter Russia in the information space, these negative aspects should be clarified more clearly. According to the Ukrainian scientist I. Lubkovych, they include:

1) inoperability (at the level of reaction to specific misinformation and information provided by Russian media networks, as well as at the level of offering own details on events and phenomena);

2) strength and Awareness. Strength is the means of conducting information warfare, and awareness - the effectiveness of their application;

3) lack of information countering public authorities;

4) finance (most media do not refuse to broadcast Russian TV shows, TV series, movies due to the financial situation and reluctance to lose money) [Лубкович 2014].

In general, the mechanisms for protecting Ukraine's information security can be divided into two groups: legislative and institutional mechanisms.

Considering *legislative mechanisms*, it should be noted that in Ukraine it has been developed a sufficient number of legal documents concerning information and information space since independence. The following Laws of Ukraine are among them: “On Information”, “On Information Agencies”, “On the Concept of the National Program of Informatization”, “On Information Protection in Information and Communication Systems”, “On the Press in Ukraine” and others [Про друковані засоби 2016; Про захист інформації 2014; Про інформаційні агентства 2015; Про інформацію 2016; Про Концепцію 2013].

The Doctrine of Information Security of Ukraine, which was recently put into effect, is one of the legislative documents concerning the information security of Ukraine. The President of Ukraine P. Poroshenko approved it on February 25, 2017 after the National Security and Defense Council approval in December 2016.

The next type of mechanisms for ensuring information security is *institutional mechanisms* that cover state and non-state institutions, whose activities are aimed at the formation and implementation of information security. Today, the subjects of the establishment and implementation of policy in the information sphere in our country include the following:

► **National Security and Defense Council of Ukraine.** The main achievements of the National Security and Defense Council in the area of information policy were the formation and adoption of the Doctrine of Information Security of Ukraine in 2017.

► **Ministry of Information Policy of Ukraine.** During the three years of its activities, the Ministry of Information Policy of Ukraine launched an Internet project “Information Forces of Ukraine”; launched Multimedia Platform for Ukraine's multilingualism; held a lot of social campaigns; collected evidence of the presence of Russian soldiers in the territory of Eastern Ukraine [Аналіз 2017].

► **Ministry of Foreign Affairs.** In general, the Ministry of Foreign Affairs of Ukraine has taken a number of actions on the way to counter Russian aggression: filed a lawsuit to the UN International Court of Justice regarding the Russian violation of the UN Convention against Terrorist Financing; made a series of statements through the delegation of Ukraine on Russian aggression against Ukraine at a meeting of the OSCE Permanent Council; monitors the situation in the occupied Crimea, etc. [Департаменти 2018; Про Доктрину 2017].

► **Ministry of Defense of Ukraine.** This central executive authority and military management are limited to powers in the information sphere concerning the

Armed Forces of Ukraine, namely: counteracting the information attacks of the aggressor directed to the Ukrainian army; assurance of authenticity and reporting of information coming to the Armed Forces of Ukraine through their media [Про Доктрину 2017].

► **The State Service of Special Communication and Information Protection of Ukraine.** It is a state body in the field of information, which is intended to ensure the formation and implementation of state policy, within its competence, in the area of information security and information protection [Про Доктрину 2017].

► **Cyber Police.** During its activity, the Cyber Police have introduced new ways to respond promptly to cybercrime; detained hundreds of online fraudsters; discovered and deactivated many Russian hacker attacks on the information systems of Ukraine, etc. [Демедюк 2015].

In our opinion, considering the mechanisms of counteraction to the Russian information warfare, one should also pay attention to the decree of the President of Ukraine P. Poroshenko about the prohibition of Russian social networks and sites, which came into force on May 17, 2017 [Про застосування 2017].

The thoughts regarding the prohibition of Russian sites and social networks divided the scientists and analysts into those who are negatively oriented to the prohibition, and those who consider this ban a great success of Ukraine in countering the Russian information warfare. Also, the reaction of international actors to the presidential decree is essential. For example, the Secretary-General of the Council of Europe, Thorbjшrn Jagland, expressed his concern about the decision, explaining that this prohibition opposes freedom of expression and freedom of the media [У Раді Європи 2017]. The same position is represented by Tanya Cooper, a representative of Human Rights Watch, who equates the decree of the President of Ukraine with the desire to control political discourse in the country from his side [Human Rights 2017].

Contrary to these positions, the Secretary-General of the North Atlantic Alliance, Jens Stoltenberg, noted that blocking by the Ukrainian government of social networks and sites of Russia is a matter of the national security of the state solely, and not for freedom of speech in it [У НАТО 2017].

It is also worth paying attention to the law about the introduction of quotas on the Ukrainian language on television, which was signed by the President of Ukraine on June 6, 2014. According to this normative act, the share of various programs, films, TV programs in Ukrainian should be at least 75 % on television. According to the President, by this decision, the Ukrainian language became protected in the middle of other languages (mainly Russian) in Ukraine [Порошенко 2017].

In our opinion, the prohibition of Russian social networks and sites, as well as the quotation of the Ukrainian language on television, are some steps towards the isolation of Ukraine from Russia. These actions of the leadership of our state show not only Russia but the whole world that Ukraine is an independent state with a single state language. However, these decisions can also have specific negative sides. The international community can consider the prohibition of Russian social networks and sites as an accurate indicator of the undemocratic nature of our state. In turn, the quotation of the Ukrainian language on television can not only create the appearance of discrimination of the Russian-speaking population in Ukraine, in which the Russian Federation convinces the whole world but also provokes the aggressor state to make some actions in response.

It should also be noted that in addition to legislative mechanisms non-state actors in Ukraine also take an active part in counteracting information warfare from the Russian Federation side. To the structures of the non-governmental sector should be attributed primarily international organizations such as the United Nations and its specialized agencies, as well as the OSCE, the Council of Europe, and others, as well as domestic civil society organizations that are actively struggling to counter Russia's information war against Ukraine.

Having considered the mechanisms of providing information security and counteracting the information threats of Ukraine, it should be noted that from 2014 Ukraine began to take specific steps to improve and ensure the effectiveness of these mechanisms. Approval of the Doctrine of Information Security of Ukraine in 2017 gave impetus to the systematization of the powers of state bodies in the field of information policy and responsibility for their non-compliance [Про Доктрину 2017]. Institutional mechanisms have expanded since 2014 thanks to the Ministry of Information Policy of Ukraine and Cyber Police. However, this is not enough in today's globalized information society. That is why Ukraine needs to analyze, develop, create and update mechanisms for countering the Russian information warfare and protecting its information security.

Russian aggression in Ukraine is by no means complete. Moreover, it is in the process of escalation. Russia accumulates its forces every day, improves its factors, and applies new technologies and methods to inflict the information blow again and again. Thus, the Russian information war will be developed and is likely to be strengthened by the use of increasingly effective tactics. It can't be said that Ukraine has already lost this war, but it still needs a lot to do to prevent this from

happening. Undoubtedly, in Ukraine, there are already many existing mechanisms for counteracting information warfare, but they need to be improved, developed and made more efficient.

The lack of sufficient state tools for conducting an information war is currently a vital issue in the war with Russia. Ukrainian scientist M. Senchenko notes that Ukraine, for its effective opposition to the information war from the side of Russia, needs to have at least: 1) an efficient system for conducting information warfare; 2) an effective concept of information warfare; 3) the strategy of performing of information warfare [Сенченко 2014].

In our opinion, the strategy of the information war of the Ukrainian state must include defense and offensive policies. Concerning the first component, then it refers to actions aimed at physical and psychological protection of the population, troops, government, information infrastructure and satellites in space. Defense policy should include: organization of the activity of the structure of the formation of defense systems and cooperation with other states in order to counter the information warfare; operational counteraction of activity, influences and manifestations of information-political aggression, operations of information-psychological war; bringing the media and virtual community associations into readiness to efficiently counteract and respond to information aggression.

In conditions when the state conducts open aggression and information warfare, as it is in relations with the Russian Federation, the operational ability to respond to various types of information attacks and threats that they carry from the side of the Russian Federation is essential.

State actions in the above conditions can be divided into three levels: the first one is geopolitical (it is the influence on the information aggressor and the limitation of the intensity and force of his attack); the second – a condition that includes the protection of the integrity, efficiency and capacity of the management system, information infrastructure, information resources; the third - the public (aimed at protecting the stability and consistency of the development of social and political relations, consciousness of citizens, the integrity of each person).

First level information policy tools should include: 1) attracting the world community and world public opinion to identify the aggressor and its devastating effects; 2) informing the world community about enemy attacks and objective state in their own country; 3) strengthening counter-propaganda, national information space, and the formation of operational information centers; 4) prohibition on the media of its territory, which belong to the information space of the aggressor, in order to avoid propaganda and destructive influence on citizens; 5) support for the stable status of the state, the positive image of Ukraine and the character of a stable state; 6) collaboration and exchange of experience with international organizations on countering cyber-attacks and information threats [Kofman 2015].

The second level, in its turn, is quite extensive and combines the system of state administration and national information infrastructure, the country's overall defense capability, its ability to withstand aggressive attacks and maintain the informational, territorial, economic, socio-political, cultural integrity of the state. The main mechanisms of informational policy should include: 1) creation of a coordinating body, decision-making center, information policy and security management, creation of a single effective system with a vertical line of organs and institutes; 2) training specialists in the field of information warfare and implementation of the state information strategy: political scientists, analysts, specialists in information technology, information-psychological security, practical psychologists on assistance to victims of information aggression; 3) training of civil servants on the principles and methods of protecting information, information literacy and the bases of information security, psychological protection of consciousness and strengthening of “information immunity”; 4) creation of a specialized body for cybersecurity and counteracting hacker attacks with the involvement of information technology specialists; 5) Management and control of internal and continuous analysis of external information fields. Improvement of the institutional component of monitoring information and legislative consolidation of the relevant activities, as well as responsibility for actions in this area; 6) creation of a single research and information center for the processing of news for a specified period to identify the sources of information, the news market and state sources of the enemy's intelligence; strengthening the information resources of political organizations; 7) Increasing of the legal responsibility of the media for the spread of destructive information, aggressive appeals, the range of hostile ideas, etc.; 8) information and psychological defense of military command and army from the propaganda of demoralization; learning methods of information protection, principles of offensive and defensive actions in response to information warfare, features of the use of information weapons [Kofman 2015].

Concerning the third level – the public – it is essential here the activity aimed at supporting the stability of socio-political development, consolidation and psychological security of citizens and mass

consciousness in general. Therefore, among the mechanisms of the third level of state political opposition should be: 1) providing citizens with necessary information, informing the public about the information dangers and information weapons, both technical and psychological;. 2) development of independent social media; 3) involvement of virtual public associations and mass media to protect the national information space, create a virtual system of collective security, and reduce social tension; 4) protection of the spiritual potential of society from imposing hostile values, increasing the stability of the consciousness of children and young people; 5) strengthening of symbolism and ideology, which is based on the principles of respect, unity, and solidarity. Creation of social videos and advertising, which should be aimed at the psychological protection of citizens [Kofman 2015].

Particular attention should be paid to the mass media in planning and implementing effective information security mechanisms and countering the Russian information warfare in Ukraine. The loss of Ukraine in the information war with Russia is in some way due to the vulnerability of the Ukrainian mass media to information attacks and misinformation from the Russian side. In general, the following causes of such weakness of Ukrainian mass media can be singled out: 1) the emergence of many new electronic resources that are aimed at anti-Ukrainian politics and are propagandistic. The problem with Ukraine in this situation is the lack of control over the emergence of such electronic resources and the prompt response to such phenomena; 2) the active appearance in the media, social networks and other informational objects of propaganda materials and the lack of control over the dissemination of this information; 3) the insufficient effectiveness of the confrontation with viruses and harmful Russian software, which is engaged in the spread of Russian propaganda, misinformation and information influence; 4) the effectiveness of the Russian Federation in the development of systems that are involved in manipulating the consciousness of citizens and the dissemination of misinformation. At the same time, Ukraine is only beginning to develop such systems; it doesn't have the means to counter driving information signals from the Russian side; 5) improper training of specialists in conducting information warfare and ensuring information security of the state. Ukraine has an insufficient number of higher education institutions that train specialists in information protection and cyber defense; 6) the insignificant amount of source base that would provide information on the specifics, means, methods, features of the information warfare and tactics of its conduct. If we analyze the availability of such literature, its number is insufficient, and the number of modern specialists on these issues – even less [Еляшевська 2015].

As we can see, the Ukrainian media space is exceptionally vulnerable to information attacks and actions by the Russian Federation and significantly loses in this confrontation. Undeniably, the key to effective counteraction to the Russian information war against Ukraine is not only Ukraine's state capacity to respond to Russian information attacks, but also international assistance from leading international actors such as the United States and the EU. The information war of Russia, as international practice shows, is not only against Ukraine. Russian hackers also interfere in the information systems of other countries, including the United States [Dibb 2016].

Summing up, it should be noted that despite the existence in Ukraine of a database of legislative mechanisms for information security and counteraction to Russia's information war against Ukraine, it is not properly formed. The modern information era is rapidly transforming and leads to the emergence of new means and methods of warfare. And Russia is ahead of Ukraine in a few steps in the development of its mechanisms and technologies. That is why the essential things for the Ukrainian state are: the formation of a genuinely efficient system of information warfare, as well as the method of counteracting information influences on the part of the aggressor state; development of information warfare strategy with the participation of scientists, political scientists and analysts specializing in the information sphere; support of the state’s image, improvement of the efficient coverage of reliable information in mass media and improvement of their work in general.

At the same time, taking into account the continuation of informational confrontation between Russia and Ukraine, our scientific study can't be considered as complete, given the variability of its object. A promising direction of our further research in this direction may be an analysis of the level of effectiveness of counteraction to the Russian information warfare against Ukraine in the future, as well as the study of international experience in the fight against information warfare.

СПИСОК ЛІТЕРАТУРИ

Аналіз роботи Міністерства інформаційної політики України за 2016 рік (2017). Отримано з: http://mip.gov.ua/files/pdf/MIP_2016_Year_report_UA.pdf.

Демедюк, С. В., Марков, В. В. (2015). Кіберполіція України. *Наше право, № 6,* 87-93.

Департаменти та управління Міністерства закордонних справ України (2018). Отримано з: http://mfa.gov.ua/ua/about-mfa/structure/staff.

Еляшевська, Н. (2015). Вразливість України до інформаційної війни. *Теле- та радіожурналістика, Vol. 14,* 165-169.

Про друковані засоби масової інформації (пресу) в Україні: Закон України № 2782-12 від 16.11.1992. зі змінами та доповненнями 08.12.2016 (2016). Отримано з: http://zakon3.rada.gov.ua/laws/show/ 2782-12

Про захист інформації в інформаційно-телекомунікаційних системах: Закон України № 80/94-ВР від 05.07.1994 зі змінами та доповненнями від 27.03.2014 (2014). Отримано з: http://zakon5.rada.gov.ua/laws/show/80/94- %D0 %B2 %D1 %80

Про інформаційні агентства: Закон України № 74/95-ВР від 28.02.1995 зі змінами і доповненнями від 09.04.2015 (2015). Отримано з http://zakon3.rada.gov.ua/laws/show/74/95- %D0 %B2 %D1 %80

Про інформацію: Закон України № 2658-12 від 02.10.1992 зі змінами і доповненнями від 06.12.2016 (2016). Отримано з http://zakon2.rada.gov.ua/laws/show/2657-12

Про Концепцію національної програми інформатизації": Закон України № 75/98-ВР від 04.02.1998 зі змінами і доповненнями від 04.07.2013 (2013). Отримано з http://zakon3.rada.gov.ua/laws/show/75/98- %D0 %B2 %D1 %80

Лубкович, І. М. (2014). Місце українських медій в інформаційній війні 2013–2014 рр. *Наукові записки інституту журналістики, № 56,* 182–187.

Порошенко підписав закон про мовні квоти (2017). *Слово і Діло.* Отримано з: https://www.slovoidilo.ua/2017/06/06/novyna/pravo/poroshenko-pidpysav-zakon-pro-movni-kvoty.

Расторгуев, С. П. (1997). Информационная война как целенаправленное информационное воздействие информационных систем. *Информационное общество, № 1,* 64-66.

Сенченко, М. (2014). Запорука національної безпеки в умовах інформаційної війни. *Вісник Книжкової палати, № 6,* 3-9.

У НАТО озвучили позицію щодо заборони російських соцмереж в Україні (2017). Отримано з: https://www.unian.ua/politics/1939549-u-nato-ozvuchili-pozitsiyu-schodo-zaboroni-rosiyskih-sotsmerej-v-ukrajini.html.

У Раді Європи стурбовані указом Порошенка про заборону російських сайтів (2017). Отримано з: https://www.rbc.ua/ukr/news/sovete-evropy-obespokoeny-ukazom-poroshenko-1495015079.html.

Про Доктрину інформаційної політики України: Указ Президента України № 47 від 25.02.2017 (2017). Отримано з: http://www.president.gov.ua/documents/472017-21374.

Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій): Указ Президента України № 133 від 28.04.2017 (2017). Отримано з: http://www.president.gov.ua/documents/ 1332017-21850.

Dibb, P. (2016). Why Russia is a threat to the international order. Retrieved from: https://www.aspi.org.au/publications/why-russia-is-a-threat-to-the-international-order/Russia.pdf.

Human Rights назвала заборону російських соцмереж та інтернет-ресурсів в Україні "страшним ударом" по свободі слова (2017). Отримано з: http://ua.interfax.com.ua/news /general/422093.html.

Kofman, M., Rojansky M. (2015). A Closer look at Russia's "Hybrid War". Retrieved from: https://www.wilsoncenter.org/sites/default/files/7KENNAN %20CABLEROJANSKY %20KOFMAN.pdf

Lamb, Ch. J. (1997). The impact of information age technologies on operations other than war. In *War in the information age: new challenges for U. S. security policy (ed. by Robert L Pfaltzgraff; Richard H Shultz).* Washington: D. C.: Brassey's, 256-268.

REFERENCES

About information: Law of Ukraine No. 2658-12 of 02.10.1992, as amended and supplemented from 06.12.2016 (2016). Retrieved from: http://zakon2.rada.gov.ua/laws/show/2657-12

About information agencies: Law of Ukraine No. 74/95-VR of February 28, 1995, as amended on April 9, 2015 (2015). Retrieved from: http://zakon3.rada.gov.ua/laws/show/74/95- %D0 %B2 %D1 %80

About printed mass media (press) in Ukraine: Law of Ukraine No. 2782-12 dated 16.11.1992 with amendments and supplements 08.12.2016 (2016). Retrieved from: http://zakon3.rada.gov.ua/laws/show/ 2782-12

About the application of personal special economic and other restrictive measures (sanctions): Decree of the President of Ukraine No. 133 dated April 28, 2017 (2017). Retrieved from: http://www.president.gov.ua/documents/ 1332017-21850.

About the Concept of the National Program of Informatization ": Law of Ukraine No. 75/98-VR of February 4, 1998, as amended and supplemented from July 4, 2013 (2013). Retrieved from: http://zakon3.rada.gov.ua/laws/show/75/98- %D0 %B2 %D1 %80

About the Doctrine of the Information Policy of Ukraine: Decree of the President of Ukraine No. 47 of 02/25/2017 (2017). Retrieved from: http://www.president.gov.ua/documents/472017-21374.

About the protection of information in telecommunication and information systems: Law of Ukraine No. 80/94-VR of July 5, 1994, as amended and supplemented by 27.03.2014 (2014). Retrieved from: http://zakon5.rada.gov.ua/laws/show/80/94- %D0 %B2 %D1 %80

Analysis of the work of the Ministry of Information Policy of Ukraine for 2016 (2017). Retrieved from: http://mip.gov.ua/files/pdf/MIP_2016_Year_report_ UA.pdf.

Demediuk, S. V., Markov, V. V. (2015). The cyber police of Ukraine. *Our right, № 6,* 87-93.

Departments and offices of the Ministry of Foreign Affairs of Ukraine (2018). Retrieved from: http://mfa.gov.ua/ua/about-mfa/structure/staff.

Dibb, P. (2016). Why Russia is a threat to the international order. Retrieved from: https://www.aspi.org.au/publications/why-russia-is-a-threat-to-the-international – order/Russia.pdf.

Eliashevska, N. (2015). Ukraine's vulnerability to information warfare. TV and radio journalism, *Vol. 14,* 165–169.

Human Rights has called the prohibition of Russian social networks and Internet resources in Ukraine "a terrible

blow to freedom of speech" (2017). Retrieved from: http://ua.interfax.com.ua/news /general/422093.html.

Kofman, M., Rojansky M. (2015). A Closer look at Russia's "Hybrid War". Retrieved from: https://www. wilsoncenter.org/sites/default/files/7KENNAN % 20CABLEROJANSKY %20KOFMAN.pd

Lamb, Ch. J. (1997). The impact of information age technologies on operations other than war. In ***War in the information age: new challenges for U. S. security policy (ed. by Robert L Pfaltzgraff; Richard H Shultz).*** Washington: D. C.: Brassey's, 256-268.

Lubkovych, I. M. (2014). Place of Ukrainian media in the informational war of 2013–2014. ***Scientific notes of the Institute of Journalism, № 56,*** 182–187.

NATO has voiced its position on the prohibition of Russian social networks in Ukraine (2017). Retrieved from: https://www.unian.ua/politics/1939549-u-nato-ozvuchili-pozitsiyu-schodo-zaboroni-rosiyskih-sotsmerej-v-ukrajini.html.

Poroshenko signed the law about language quotas (2017). ***Word and Matter.*** Retrieved from: https://www. slovoidilo.ua/2017/06/06/novyna/pravo/poroshenko-pidpysav-zakon-pro-movni-kvoty.

Rastorhuev, S. P. (1997). Information war as a purposeful information impact of information systems. ***Information society, № 1,*** 64–66.

Senchenko, M. (2014). The key to national security in the context of information warfare. ***Announcer of the Book Chamber, № 6,*** 3–9.

The Council of Europe is concerned about the ban on Russian sites by Poroshenko's decree (2017). Retrieved from: https://www.rbc.ua/ukr/news/sovete-evropy-obespokoeny-ukazom-poroshenko-1495015079.html.